Fusion of LSB and DWT Biometric Watermarking Using Offline Handwritten Signature for Copyright Protection

Cheng-Yaw Low[1], Andrew Beng-Jin Teoh[2], and Connie Tee[1]

[1] Faculty of Information Science and Technology
Multimedia University, Jalan Ayer Keroh Lama, 75450 Melaka, Malaysia
{cylow,tee.connie}@mmu.edu.my
[2] Electrical and Electronic Engineering Department
Yonsei University, Seoul, South Korea
bjteoh@yonsei.ac.kr

Abstract. Biometric watermarking was introduced as the synergistic integration of biometrics and digital watermarking technology. This paper proposes a novel biometric watermarking technique, which embeds offline handwritten signature in host image for copyright protection. We propose to combine the conventional LSB-based and DWT-based watermarking techniques into a unison framework, which is known as LSB-DWT in this paper. The proposed LSB-DWT technique is evaluated against various simulated security attacks, i.e. JPEG compression, Gaussian low-pass filtering, median filtering, Gaussian noise, scaling, rotation and cropping. The experimental results demonstrate that the proposed LSB-DWT technique exhibits remarkable watermark imperceptibility and watermark robustness.

Keywords: Biometric watermarking, offline handwritten signature, copyright protection.

1 Introduction

Digital watermarking is the practice of concealing additional information in digital document, e.g. image, audio, video, etc, which is generally termed as host. The host is traditionally embedded with originator's name, graphical logo, serial number, binary bitstring, etc, which are coined as conventional watermark henceforward, to prosecute copyright infringements. The major drawback of the conventional watermark is that it lacks the non-repudiation property as anyone including malicious users can embed a particular name or logo in the host.

Biometrics, which measures human physiological and behavioural characteristics, e.g. fingerprint, iris, hand geometry, face, handwritten signature, etc, provides unique means to recognise a person. In recent years, biometrics is synergistically merged into the digital watermarking technology to replace the conventional digital watermarking techniques. This advancement can be categorized as follows:

M. Tistarelli and M.S. Nixon (Eds.): ICB 2009, LNCS 5558, pp. 786–795, 2009.

i. Watermarked Biometrics - The host is a biometrics, whereas the watermark can either be a biometrics, or other proprietary notice. For example, biometrics, e.g. fingerprint, iris, or demographic information, e.g. name, etc, can be embedded in the biometric host to protect against biometric template theft. In addition, there are some cases where the biometric host only acts as a carrier of genuine biometrics. In such cases, the genuine biometrics can be highly protected as the intruders might not be aware that the biometric host is invisibly attached with the genuine biometrics.
ii. Biometric Watermarking - This category employs biometrics as the watermark, whereas the host can be any copyrighted documents. Since biometrics provides uniqueness which can hardly be counterfeited, misplaced, or shared, biometric watermarking promises stringent security against fraudulent watermark.

Biometric watermarking was first proposed by Jain in year 2002. Jain and Uludag [5] suggested an amplitude modulation-based biometric watermarking technique for two application scenarios. In the first scenario, fingerprint minutiae were embedded in fingerprint, face and arbitrary images, which were merely acting as a carrier to secure the genuine fingerprint minutiae. In the next application scenario, fingerprint minutiae were embedded in face image, and the watermarked face image was then encoded in smart card. To authenticate the smart card holder, his/her fingerprint was captured and matched against the fingerprint minutiae stored in the smart card. On the other hand, Jain et al. [4] proposed a biometric watermarking technique to embed a person's face code in his/her fingerprint image. The extracted face code was used as an additional source, besides the fingerprint image, to verify the system users. Namboodiri and Jain [6] recommended a biometric watermarking technique to embed online handwritten signature in host image. The Equal Error Rate (EER) of Namboodiri's technique was reported to be approximately 7%. In spite of that, Namboodiri's technique is highly fragile towards further image manipulations, e.g. JPEG compression, image filtering, etc. Hassanien [7] introduced a Discrete Wavelet Transform (DWT)-based biometric watermarking technique to embed iris code in host image. However, the credibility of Hassanien's technique was only evaluated against JPEG compression.

The conventional Least Significant Bit (LSB)-based and DWT-based techniques are recently fused into a unison framework, which is abbreviated as LSB-DWT. Chen and Wang [3] applied integer-to-integer DWT to transform host image into equivalent DWT domain of integer coefficients, and watermark was embedded in 5-bit of DWT coefficients based on exclusive-OR operation. The shortcoming of integer-to-integer DWT is that it involves round-off function which might eliminate the watermark. The proposed LSB-DWT technique exploits conventional DWT to decompose host image into DWT domain, and offline handwritten signature, i.e. still signature image, is then repeatedly embedded in 5-bit of DWT coefficients for copyright protection. The most significant advantage of handwritten signature over other biometric attributes is that it has traditionally been used for authenticating official documents and thus it is socially accepted.

2 Biometric Watermarking

Fig. 1 shows the generic diagram of the proposed LSB-DWT technique. In general, it encompasses of four main modules:

i. Pre-processing, Feature Extraction, and Discretisation - To use signature image as watermark, it is first transformed into binary bitstring, which is referred to as signature code in this paper. Since the signature image might contain scratches, speckles, smears, or other unwanted artefacts that can thwart feature extraction, it is smoothed using median filtering. The signature image is then converted to binary image of 300 x 200 pixels to isolate the signature from the background. Subsequently, the signature image is projected into feature space via Discrete Radon Transform (DRT). As DRT produces feature space of high dimension, Principle Component Analysis (PCA) is applied to compress the DRT feature space while retaining the major characteristics. The PCA feature space is lastly discretised into the signature code of N bits, where N is set to 10, 50, and 100, based on Kevenaar et al. [8].
ii. Watermark Embedding - The signature code is embedded in the host image to establish the host authenticity (refer Section 3.3). Typically, one or more secret keys are required to safeguard the signature code. This is due to the reason that the watermarked host image can be exposed to a wide range of security attacks, e.g. JPEG compression, image filtering, rotation, scaling, etc, through insecure distribution channels.
iii. Watermark Extraction - The signature code is extracted from the watermarked host image based on the secret keys used in the watermark embedding module (refer Section 3.4).
iv. Matching - The extracted signature code is compared to the original template stored in the database to validate the host authenticity. The extracted signature code is accepted as genuine, or rejected as fraudulent based on an empirical threshold.

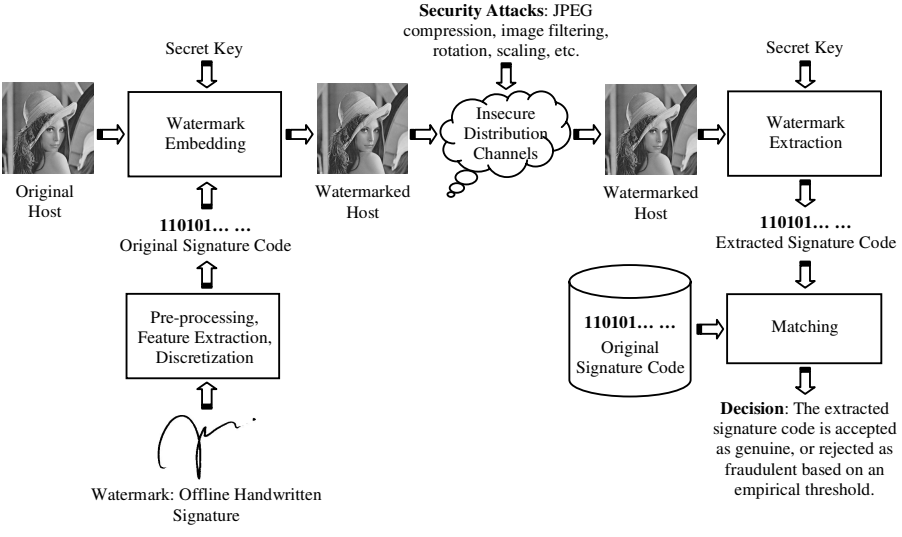

Fig. 1. Generic diagram of the proposed LSB-DWT technique

In accordance with Hartung and Martin [2], a fundamental biometric watermarking technique should at least possess the following requirements:

i. Watermark Imperceptibility - The watermark should be transparent from visual inspection, where both of the original and the watermarked host images should be indistinguishable in terms of host fidelity.
ii. Watermark Robustness - The watermark should be resistant to security attacks, where the extracted watermark should contain zero, or negligible distortion.
iii. Watermark Capacity - The watermark should convey as much information as possible.
iv. Watermark Security - The watermark should only be accessible by authorized parties. This can be achieved using cryptographic keys.

3 Proposed LSB-DWT Technique

3.1 Least Significant Bit

The least significant bit (LSB) denotes the right-most bit of a given binary number, which conveys the least important information; on the other hand, the most significant bit (MSB) is the left-most bit of the binary number, which conveys the most important information. Fig. 2 depicts the 8-bit binary representation of 149, where the MSB and the LSB correspond to the values of 128 and 1, respectively.

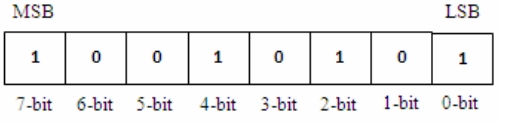

Fig. 2. 8-bit binary representation of decimal 149

The conventional LSB-based watermarking technique embeds the watermark in the LSB of the host pixels. As the LSB is the most insignificant as compared to other bits, the watermark can be embedded in the host image without corrupting the host fidelity. In spite of that, LSB-based technique is highly fragile against security attacks. This is because the watermark can be distorted or damaged if the watermarked host image is exposed to the common image manipulations, e.g. JPEG compression, image filtering, etc. Instead of the LSB, the watermark can be embedded in the *l*-bit, except the MSBs (the bits closest to, and including the MSB), to improve watermark robustness. This is due to the fact that the MSBs are the most significant and thus there are very sensitive to modification.

3.2 Discrete Wavelet Transform

Discrete Wavelet Transform (DWT) transforms the host image into four frequency sub-bands of equal sizes at each decomposition level n, namely an approximation sub-band (LL_n) and three detailed sub-bands (HL_n, LH_n and HH_n). The approximation sub-band refers to the low frequency sub-band, which can be down-sampled into multiple levels to obtain the next coarser domains. In contrast, the detailed sub-bands represent

the middle and the high frequency sub-bands, which are the finest and thus additional down-sampling is prohibited.

As the approximation sub-band consists of the salient attributes of the host image, e.g. smooth variation region, the watermark can be embedded in this sub-band to gain extra watermark robustness. However, a trade-off exists where the host fidelity can be degraded, or corrupted at the worst. The detailed sub-bands contain the image details, e.g. edges and textured regions, which are less significant and therefore less sensitive to the host fidelity. Rather than HH_n, the watermark is typically embedded in HL_n and LH_n as HH_n is susceptible to security attacks. Depending on the intended applications, the watermark can still be embedded in HH_n.

3.3 Proposed LSB-DWT Watermark Embedding Technique

The proposed LSB-DWT technique is an adaptive fusion of the conventional LSB-based and DWT-based technique. In general, the watermark, i.e. signature code in this paper, is embedded in the selected DWT coefficients of the host image using the LSB substitution technique. Let the signature code S is of N bits as follows:

$$S = [s_0, s_1, s_2, \ldots, s_{N-1}],\ s_i \in \{0,1\}.$$

where N is set to 10, 50 and 100 bits; the host image is decomposed into equivalent 3-level DWT domain and a pseudorandom number generator is initialised using a secret key k to select N random coefficients C from HL_3 and LH_3 sub-bands with respect to an empirical threshold t as follows:

$$C = [c_0, c_1, c_2, \ldots, c_{N-1}],\ C > t,\ C \in \{HL_3, LH_3\}.$$

The proposed LSB-DWT technique embeds s_i in the integer part of c_i. Assume c_i is the selected coefficient of value 149.1258; the integer part, i.e. 149, is converted to 8-bit binary representation, and the fractional part, i.e. 0.1258, is temporary stored (see Fig. 3(a)). Assume also s_i is a bit '1' (see Fig. 3(b)); the bit '1' is inserted in the 5-bit of the binary number to construct the watermarked binary number. The watermarked binary number is then reconverted back to the decimal representation, and the original fractional part, i.e. 0.1258, is reinstated to obtain the watermarked coefficient of value 181.1258. This process is repeated until the signature code is completely embedded in the host image. In the experiments, s_i is repeatedly embedded in the host image for 10 times to improve watermark robustness. At last, 3-level inverse DWT is performed to generate the watermarked host image.

3.4 Proposed LSB-DWT Watermark Extraction Technique

To extract the signature code, the watermarked host is decomposed into its 3-level DWT domain. After that, the watermarked coefficients C' are identified from HL_3' and LH_3' sub-bands by reusing the secret key k as follows:

$$C' = [c_0', c_1', c_2', \ldots, c_{N-1}'],\ C' \in \{HL_3', LH_3'\}.$$

Let c_i' be the watermarked coefficient of value 181.1258 (see Fig. 4); the integer part, i.e. 181, is converted to 8-bit binary representation, and the 5-bit is assumed to be the extracted signature code s_i'. As the signature code is embedded in the host image for multiple times, s_i' is determined by finding the most frequent occurrence bit (mode).

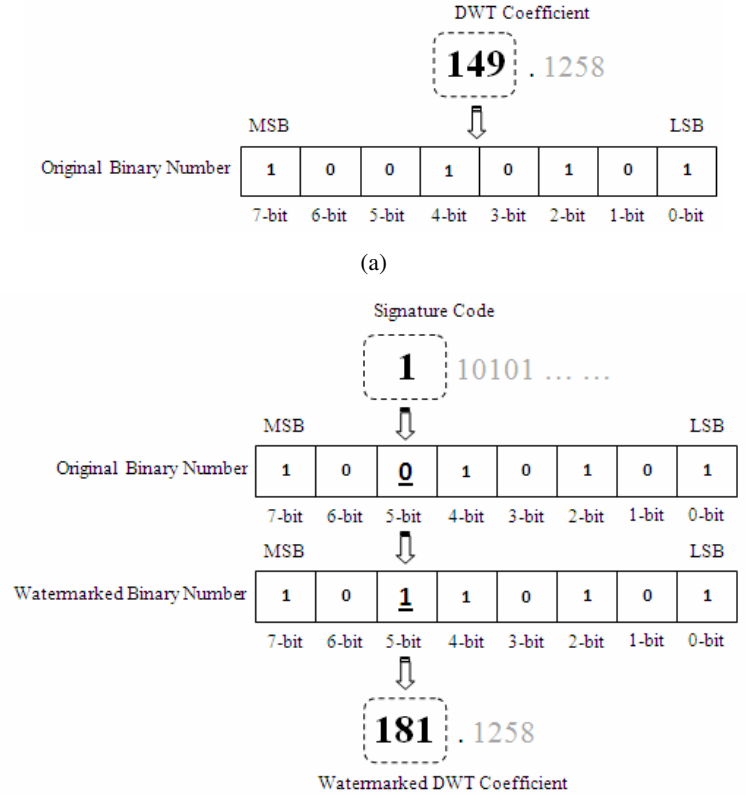

Fig. 3. Generic diagram of the proposed LSB-DWT watermark embedding technique

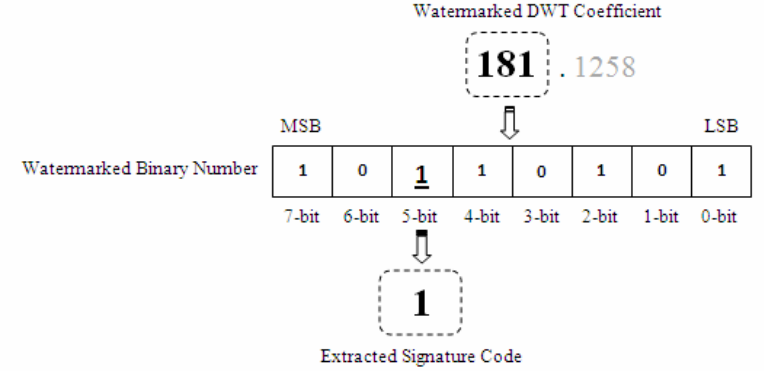

Fig. 4. Generic diagram of the proposed LSB-DWT watermark extraction technique

4 Performance Evaluation

A signature database, which consists of 500 offline handwritten signatures obtained from 50 signatories, has been constructed for performance evaluation. Unlike other biometric attributes such as fingerprint, iris, hand geometry, face, etc, the handwritten signature is a behavioural attribute, which has certain degree of intra-class variation due to age, illness, emotional state and geographical location of the signatory. This implies that there is no handwritten signature with the exact signing style although it can be provided by the same signatory. Hence, signature acquisition was completed within two contact sessions. During the first contact, each signatory was requested to provide 5 handwritten signatures. One week after the first contact, each signatory was again requested to provide another 5 handwritten signatures. All acquired handwritten signatures were then scanned and transformed into signature code of 10, 50, and 100 bits. Throughout the experiments, a gray-level Lena image was adopted as the host image. It was formatted in bitmap with the size of 512 x 512 pixels.

4.1 Performance Criteria

The performance of the proposed LSB-DWT technique was investigated in terms of watermark imperceptibility and watermark robustness.

Watermark Imperceptibility. Due to the fact that human eyes can tolerate different degree of distortion, a quantitative index, i.e. Peak Signal to Noise Ratio (PSNR), is adopted to estimate the dissimilarity between the original and the watermarked host images. Let I_{ori} and I_w denote the original and the watermarked host images of m x n pixels, respectively; PSNR can be defined via Mean Square Error (MSE) in the unit of logarithmic decibel (dB) as follows:

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right), \text{where } MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\left[I_{ori}(i,j) - I_w(i,j)\right]^2 .$$

PNSR only provides a rough estimation of the watermarked host image, irrespective of its host fidelity. A higher PSNR indicates that the watermarked host image is closer to the original one from the perspective of host contents. In accordance with Chen et al. [1], the host fidelity is acceptable for any PSNR greater than 30 dB.

Watermark Robustness. A number of security attacks were simulated to validate the watermark robustness of the proposed LSB-DWT technique, which include:

i. JPEG Compression - The host image was compressed using JPEG compression of JPEG quality ratio 80%, 50% and 20%.
ii. Gaussian Low-pass Filtering - The host image was filtered using Gaussian low-pass filter of 3 x 3 neighbourhood and standard deviation of 0.5.
iii. Median Filtering - The host image was distorted using median filtering of 3 x 3 neighbourhood.
iv. Gaussian Noise - The host image was added with Gaussian noise of zero-mean and variance of 0.01.
v. Scaling - The host was shrunk to 128 x 128 pixels using the nearest neighbour interpolation method, and is then rescaled back to its original size.

vi. Rotation - The host image was rotated by 10^0 in counter-clockwise direction using the nearest neighbour interpolation method, and is then rotated by 10^0 in clockwise direction to restore the host image back to its initial orientation.
vii. Cropping - A pre-determined area was cropped from the host image to simulate data reduction attack.

The distortion rate of the extracted signature code was measured after the host image was subjected to the simulated security attacks using normalized Hamming distance:

$$\varepsilon(S, S') = \frac{\sum S \oplus S'}{N}.$$

where S and S' denote the original and the extracted signature code, respectively, and N refers to the signature code length of 10, 50, or 100 bits. In the experiments, the extracted signature code is assumed to be damaged if the distortion rate exceeds 0.50.

5 Experimental Results

Table 1 summarizes the experimental results of the proposed LSB-DWT technique. It reveals that PSNR is inverse-proportional to the signature code length N. However, the proposed LSB-DWT technique is demonstrated to be capable of safeguarding the host fidelity from severe degradation as PSNR for N = 10; 50; 100 are at least 45dB. Furthermore, Fig. 5 illustrates that the watermarked host image of the proposed LSB-DWT technique for N = 100 is still close the original one. Table 1 also reveals that the proposed LSB-DWT technique is extremely robust against JPEG 80%, JPEG 50%, Gaussian low-pass filtering, median filtering, rotation and cropping, as the signature code can be fully extracted. Meanwhile, JPEG 20%, Gaussian noise, and scaling are proven to be able to deform the signature code insignificantly.

The proposed LSB-DWT technique is compared with the conventional LSB-based technique, Hassanien's technique in [7], and Chen's techniques in [3]. In general, Hassanien technique is a DWT-based method, which embeds the iris code in the host image based on the proposed quantization rules. On the other hand, Chen's technique is also a fusion of the conventional LSB-based and DWT-based techniques, which

Table 1. Experimental results of the proposed LSB-DWT technique

The Proposed LSB-DWT Technique			
Signature Code Length (*N* bits)	**10**	**50**	**100**
PSNR (dB)	55.8463	49.0162	45.9280
Simulated Security Attacks	**Distortion Rate**		
No Attack	0.0000	0.0000	0.0000
JPEG 80%	0.0000	0.0000	0.0000
JPEG 50%	0.0000	0.0000	0.0000
JPEG 20%	0.0000	**0.0200**	**0.0100**
Gaussian Low-Pass Filtering	0.0000	0.0000	0.0000
Median Filtering	0.0000	0.0000	0.0000
Gaussian Noise	0.0000	0.0000	**0.0200**
Scaling	0.0000	0.0000	**0.0300**
Rotation	0.0000	0.0000	0.0000
Cropping	0.0000	0.0000	0.0000

Fig. 5. Watermarked host image of the proposed LSB-DWT technique for N = 100

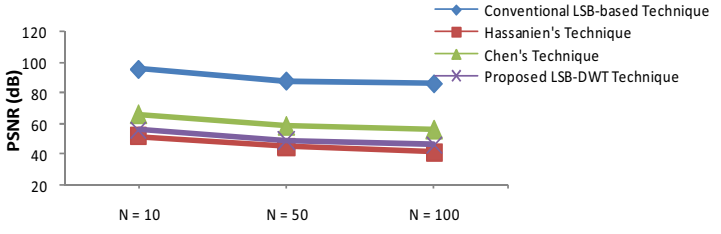

Fig. 6. PSNR comparison between the conventional LSB-based, Hassanien's, Chen's, and the proposed LSB-DWT techniques

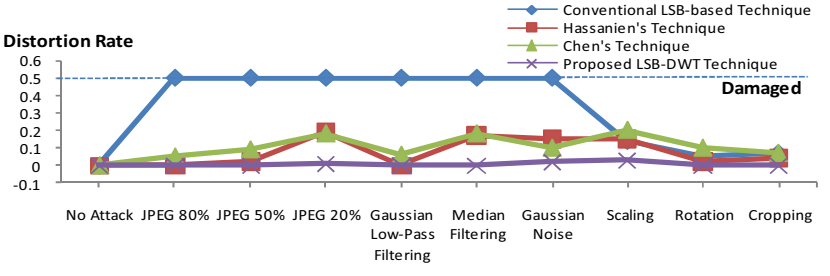

Fig. 7. Distortion comparison between the conventional LSB-based, Hassanien's, Chen's, and the proposed LSB-DWT techniques for N =100

exploits integer-to-integer DWT to transform the host image into DWT domain. The watermark is then embedded in the 5-bit of the selected DWT coefficients based on exclusive-OR operation.

Fig. 6 depicts the PSNR distributions of the conventional LSB-based, Hassanien's, Chen's, and the proposed LSB-DWT-based techniques. It is clearly demonstrated that the conventional LSB-based technique is outstanding in safeguarding the host fidelity.

According to Fig. 7, the conventional LSB technique is revealed to be fragile against JPEG compression, Gaussian low-pass filtering, median filtering, and Gaussian noise. This is because the LSB consists of the least significant components which

are highly vulnerable to frequency-based operations. Despite Hassanien's technique outperforms the conventional LSB technique, it still lacks the desired robustness to protect the signature code from distortion. In addition, Fig. 7 also reveals that the proposed LSB-DWT technique is superior to Chen's technique. This is due to the reason that Chen's technique uses integer-to-integer DWT, which involves round-off function. Thus, the signature code can be unintentionally eliminated. Apart from that, the proposed LSB-DWT technique uses redundant watermarking scheme, which is capable of improving the watermark robustness.

6 Conclusion

This paper proposes a novel biometric watermarking technique, which is referred to as LSB-DWT technique, to embed offline handwritten signature in copyrighted host image as the claim of rightful ownership. A variety of security attacks are simulated to investigate the watermark robustness of the proposed LSB-DWT technique, which include JPEG compression, Gaussian low-pass filtering, median filtering, Gaussian noise, scaling, rotation, and cropping. Experimental results show that the proposed LSB-DWT technique is proficient in protecting the host fidelity, and is sufficiently robust against the simulated security attacks.

Acknowledgements

This work was supported by the Korea Science and Engineering Foundation (KOSEF) through the Biometrics Engineering Research Center (BERC) at Yonsei University (Grant Number: R112002105080020(2008)).

References

1. Chen, T.S., Chang, C.C., Hwang, M.S.: A Virtual Image Cryptosystem based upon Vector Quantization. IEEE Transactions on Image Processing 7, 1485–1488 (1998)
2. Hartung, F., Kutter, M.: Multimedia Watermarking Technique. IEEE Transactions - Invited Paper 87(7), 1079–1107 (1999)
3. Chen, T., Wang, J.C.: Image Watermarking Method using Integer-to-Integer Wavelet Transform. Tsinghua Science and Technology 7(5), 508–512 (2002)
4. Jain, A.K., Uludag, U., Hsu, R.L.: Hiding a Face into a Fingerprint Image. In: IEEE International Conference on Pattern Recognition (2002)
5. Jain, A.K., Uludag, U.: Hiding Biometric Data. IEEE Transactions on Pattern Analysis and Machine Intelligence 25(11), 1494–1498 (2003)
6. Namboodiri, A.M., Jain, A.K.: Multimedia Document Authentication using On-line Signatures as Watermarks. In: Proceedings of SPIE on Security, Steganography and Watermarking of Multimedia Content VI, vol. 5306, pp. 653–662 (2004)
7. Hassanien, A.E.: Hiding Iris Data for Authentication of Digital Images using Wavelet Theory. Pattern Recognition and Image Analysis 16(4), 637–643 (2005)
8. Kevenaar, T.A.M., Schrijen, G.J., Van der Veen, M., Akkermans, A.H.M.: Face Recognition with Renewable and Privacy Preserving Binary Templates. In: IEEE Workshop on Automatic Identification Advanced Technologies, pp. 21–26 (2005)